Army Regulation 25–1
Army Knowledge Management and Information Technology Management
30 June 2004

(Excerpts)

See http://www.usapa.army.mil/pdffiles/r25_1.pdf to view the entire regulation.

p. 27
5–11. Army Web Risk Assessment Cell (AWRAC)

The Army Web Risk Assessment Cell (AWRAC) is responsible for reviewing the content accessible Web sites. The AWRAC conducts ongoing operational security and threat assessments (.mil and all other domains used for communicating official information) to ensure that they are and Army policies and best practices. The AWRAC will—

a. Conduct random sampling of Web sites to identify security concerns or review Web site concerns Joint Web Risk Assessment Cell (JWRAC) or Army leadership.

b. Ensure inappropriate security and personal information is removed from publicly accessible

c. Ensure that Army sites are compliant with other Federal, DOD, and Army Web site administration example, Government Information Locator Service (GILS) registration). (See also para 6–4*n*.)

d. Notify the Web site owner with operational responsibility and the IAPMs of the respective the violations and suspense dates for reporting corrective action.

e. As required, report deficiencies and corrections to the Army CIO/G–6 and JWRAC.

…

Pgs. 39-41
6–4.

…

n. Internet (World Wide Web (WWW)), intranets, and extranets. Official Army Web sites may exist on any of the above forms of "nets." The use of these net communications can support execution of Army missions through information sharing and save resources currently expended on traditional means of communication. Users are encouraged to make it their preferred and routine choice to access, develop, and exchange information. Army Web sites must be in compliance with the DOD Web site administration policy or contained within subsequent DOD directives. The following Army policies also apply:

(1) Access to all forms of nets is authorized according to the controls applied by the Web site owners.

(2) AKO is the enterprise portal for Army unclassified intranets and the NIPRNET.

AKO is the single Army portal for authenticating users to gain access to Army systems and Web servers Existing Army portals or Web servers with authentication services will migrate authentication support to AKO unless waived by CIO/G–6. The AKO–S is the enterprise portal for classified intranets and the SIPRNET. The use of AKO and AKO–S enables optimal sharing of Army information and knowledge resources across the entire Army enterprise. Army activities will maximize their use of AKO resources, features,

and tools in order to reduce the need for installation and MACOM investment in the same types of IT resources.

(a) Army Web-enabled business applications are required to be linked to the AKO portal. Initial minimum standard to link applications to AKO is a URL link on the Army portal. The objective standard to link applications to AKO is to use the AKO directory services for authentication as well as a URL link on the Army portal.

(b) Proponents are required to establish the appropriate mechanisms to protect sensitive information from being accessed by unauthorized individuals. AKO is responsible for generating user IDs and accounts, performing authentication via secure Lightweight Directory Access Protocol (LDAP) directory services, publishing updates to the technical mechanism used for directory services, and incorporating appropriate security measures. All applications, Web sites, and messaging services will use the AKO LDAP to authenticate users unless the CIO has granted a waiver.

(c) For organizational space on the AKO portal, organizations will assign a community page administrator for their primary community presence, and, where needed, assign additional administrators or other personnel to manage the content on the Knowledge Collaboration Center.

(3) NETCOM/9th ASC manages the "army.mil" Web site assignment of subdomains requested by other Army organizations. NETCOM/9th ASC promulgates procedures for Army subdomain managers, to include assignment, formatting, and any centralized registration of addresses for servers, gateways, organizations, and individual users.

(4) Because the Internet is a public forum, Army organizations will ensure that the commander, the public affairs officer (PAO), and other appropriate designee(s) (for example, command counsel, force protection, intelligence, and so on) have properly cleared information posted to the WWW or to the AKO in areas accessible to all account types. Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the WWW. (See also para 5–10.) The designated reviewer(s) will conduct routine reviews of Web sites on a quarterly basis to ensure that each Web site is in compliance with the policies herein and that the content remains relevant and appropriate. The minimum review will include all of the Web site management control checklist items at appendix C, paragraph C–4. Information contained on publicly accessible Web sites is subject to the policies and clearance procedures prescribed in AR 360–1, chapter 5, for the release of information to the public. In addition, Army organizations using the WWW will not make the following types of information available on publicly accessible Web sites:

(a) Classified and restricted or limited distribution information.

(b) FOUO information.

(c) Unclassified information that requires special handling (for example, Encrypt For Transmission Only, Limited Distribution, and scientific and technical information protected under the Technology Transfer Laws).

(d) Sensitive information such as proprietary information, predecisional documents, and information that must be protected under legal conditions such as the Privacy Act.

(e) FOIA-exempt information. Lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization, or office in the DA are prohibited on the WWW. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their

positions and duties—such as general officers and senior executives, PAOs, or other personnel designated as official command spokespersons—is permitted.

(f) Documents or information protected by a copyright.

(g) Draft publications (see also para 9–2.)

(5) The Army CIO/G–6 will provide policies, procedures, and format conventions for Web sites and will promulgate such guidance in this regulation and on the Army Web site at http://www.army.mil/webmasters/.

(6) Army organizations will assign a Web master/maintainer for each of their Web sites. Army organizations will provide their Web masters/maintainers sufficient resources and training. Web masters/maintainers will have technical control over updating the site's content and will ensure the site conforms to Defense- and Army-wide policies and conventions.

(7) Organizations maintaining publicly accessible Web sites must:

(a) Register the fully qualified domain name, (for example, http://www.us.army.mil or http://www.apd.army mil) for Army sites with the GILS and update the contact information annually. (GILS is used to identify public information resources throughout the U.S. Federal Government.)

(b) Ensure that Web servers are IAVA compliant and are placed behind a reverse proxy server or implement an alternative security procedure.

(8) Organizations requiring private Web sites (for example, intranets, extranets) must register them with the NETCOM/9th ASC Theater Network Operations and Security Center (TNOSC) and assure that the secure sockets layer (SSL) is enabled and that PKI encryption certificates are loaded. Use of Internet protocol restriction by itself is insufficient; such sites will be considered publicly accessible rather than private. PKI Web server certificates may be obtained from the NETCOM/9th ASC TNOSC.

(a) All Web applications will use AKO LDAP to authenticate clients, unless waived by NETCOM/9th ASC.

(b) All unclassified, private Army Web servers will be enabled to use DOD PKI certificates for server authentication and client/server authentication. The following type of Web server is exempt from this mandate: any unclassified Army Web server providing nonsensitive, publicly releasable information resources categorized as a private Web server only because it limits access to a particular audience only for the purpose of preserving copyright protection of the contained information sources, facilitating its own development, or restricting access to link(s) to limited access site(s) (and not the information resources).

(9) To ensure ease of access, public Web sites that collect sensitive but unclassified information from the general public as part of their assigned mission are authorized to use approved commercially available certificates to provide SSL services. Select from the trusted and validated products lists on DISA's Web site.

(10) Every Army organization that maintains a Web site must observe Federal, Defense, and Army policies for protecting personal privacy on official Army Web sites and must establish a process for webmasters/maintainers to routinely screen their Web sites to ensure compliance. At a minimum, Web sites must comply with the following Web privacy rules:

(a) Web masters/maintainers will display a privacy and security notice in a prominent location on at least the first page of all major sections of each Web site.

(b) Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used. For an example, see the Defenselink (official Web site of DOD). For management purposes, statistical summary information or other nonuser identifying information may be gathered for the purposes of assessing usefulness of information, determining technical design specifications, and identifying system performance or problem areas.

(c) Persistent "cookies" that track users over time and across different Web sites to collect personal information are prohibited on public Web sites. The use of any other automated means to collect personally identifying information on public Web sites without the express permission of the user is prohibited. Requests for exceptions must be forwarded to the Army CIO/G–6.

(d) Third party cookies will be purged from public Web sites.

(11) All Army private (nonpublicly accessible) Web sites must be located on a ".mil" domain.

(12) Web masters/maintainers will provide a redirect page when the URL of the Web site is changed.

(13) Army organizations maintaining Web sites are required to achieve Web site compliance with the provisions of Section 508 of the Rehabilitation Act Amendments of 1998 (29 USC 794d). Web sites must be equally accessible to disabled and nondisabled Federal employees and members of the public. Guidance on Section 508 standards concerning Web-based, Intranet, and Internet information and applications is located at http://www.access-board.gov/sec508/508standards.htm. Exceptions should be referred to the Staff Judge Advocate for legal review. (See also paras 6–1*p* and *q* on information access.)

(14) Internet Web sites published and sponsored by Army commands but hosted on commercial servers (servers other than "army.mil") are considered official sites and are subject to this policy.

(15) Army commands and activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web sites. Guidelines should consider the information needs of personnel and their families, mission-related needs, and public communications and community relations objectives. No compensation of any kind may be accepted in exchange for a link placed on an organization's publicly accessible official Army Web site. Listings of Web links on Army Web pages must separate external Web links from Government and military links. When external links to non-Government Web sites are included, the following disclaimer must appear on the page(s) listing external links or through an intermediate "exit notice" page: "The appearance of external hyperlinks does not constitute endorsement by the U.S. Army of this Web site or the information, products, or services contained therein. For other than authorized activities such as military exchanges and MWR sites, the U.S. Army does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this Web site."

(16) Internet Web site owners notified by the AWRAC of a violation will close the Web site or link until corrections have been completed. (See para 5–11 for additional information.)

…

p. 68
9-2. Central configuration management.
…
b. The Army Publishing Directorate manages the two official Web sites for Army-wide administrative publications and forms. Those activities desiring to provide Internet access to departmental publications and forms on a Web site must establish electronic links to the approved official publications and forms as listed in the official repository instead of publishing a duplicate publication.
…

Appendix A
References
Section I
Required Publications
…

29 U.S.C. 794d Section 508 of the Rehabilitation Act Amendments of 1998, as amended by section 2405 of the FY 2001 Military Appropriations Act (Public Law 106-246)(29 U.S.C. 794d). (Cited in para 6-3.)

…
AR 360–1 Army Public Affairs
…
Appendix C
p. 86-87
Management Control Evaluation Checklist
C–4. Test questions
e. 24-35
…
(24) Does each Web site contain a clearly defined purpose statement that supports the mission of the organization? (All)
(25) Are users of each publicly accessible Web site provided with privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service? (All)
(26) If applicable, does this Web site contain a disclaimer for external links notice for any site outside of the official DOD Web information service (usually the .mil domain)? (All)
(27) Is this Web site free of commercial sponsorship and advertising? (All)
(28) Is the Web site free of persistent cookies or other devices designed to collect personally identifiable information about Web visitors? (All)
(29) Is each Web site made accessible to handicapped users in accordance with Section 508 of the Rehabilitation Act? (All)
(30) Is operational information identified below purged from publicly accessible Web sites? (All)
(a) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.

(b) Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

(c) Personal information about U.S. citizens, DOD employees, and military personnel, to include the following:

— Social security account numbers.
— Dates of birth.
— Home addresses.
— Directories containing name, duty assignment, and home telephone numbers.
— Names, locations, or any other identifying information about family members of DOD employees or military personnel.

(d) Technological data such as—

— Weapon schematics.
— Weapon system vulnerabilities.
— Electronic wire diagrams.
— Frequency spectrum data.

(31) Are operational security tip-off indicators in the following categories purged from the organization's publicly accessible Web site? (All)

(a) Administrative.

— Personnel travel (personal and official business).
— Attendance at planning conferences.
— Commercial support contracts.
— FOUO.

(b) Operations, plans, and training.

— Operational orders and plans.
— Mission-specific training.
— Exercise and simulations activity.
— Exercise, deployment or training schedules.
— Unit relocation/deployment.
— Inspection results, findings, deficiencies.
— Unit vulnerabilities or weaknesses.

(c) Communications.

— Spectrum emissions and associated documentation.
— Changes in activity or communications patterns.
— Use of Internet and/or e-mail by unit personnel (personal or official business).
— Availability of secure communications.
— Hypertext links with other agencies or units.
— Family support plans.
— Bulletin board/messages between soldiers and family members.

(d) Logistics/maintenance.

— Supply and equipment orders/deliveries.
— Transportation plans.
— Mapping, imagery, and special documentation support.
— Maintenance and logistics requirements.
— Receipt or installation of special equipment.

(32) Has the Web site reviewer performed a key word search for any of the following documents and subsequently removed sensitive personal or unit information from publicly accessible Web sites? (All)
— Deployment schedules.
— Duty rosters
— Exercise plans.
— Contingency plans.
— Training schedules.
— Inspection results, findings, deficiencies.
— Biographies.
— Family support activities.
— Phone directories.
— Lists of personnel.
(33) Are existing infostructure capabilities and assets considered prior to upgrading, improving, or modernizing? (HQDA, MACOM)
(34) Is the fully qualified domain name (for example, http://www.us.army.mil or http://apd.army.mil) for Army sites registered with the GILS at http://sites.defenselink.mil/, and the contact information updated? (All)
…

Abbreviations:
…
AKO
Army Knowledge Online

AKM
Army Knowledge Management

AWRAC
Army Web Risk Assessment Cell

DISA
Defense Information Systems Agency

FOUO
For Official Use Only

FOIA
Freedom of Information Act

GILS
Government Information Locator Service

IAVA
Information Assurance Vulnerability Alert

LDAP
Lightweight Directory Access Protocol

MACOM
major Army command

NETCOM
U.S. Army Network Enterprise Technology Command

NIPRNET
Unclassified but Sensitive Internet Protocol Router Network

OPSEC
Operational Security

PAO
public affairs officer

PKI
Public Key Infrastructure

SIPRNET
Secret Internet Protocol Router Network

SSL
Secure Sockets Layer

TNOSC
Theater Network Operations and Security Center

URL
Uniform Resource Locator

WWW
World Wide Web
…
Section 2

Terms:
…
Access control mechanism
This permits managers of a system to exercise a directing or restraining influence over the behavior, use and content of a system. It permits management to specify what users can do, which resources they can access and what operations they can perform.

Army Knowledge Management

The Army-wide effort to transform the Army into a net-centric self-learning organization that will improve operational and mission performance.

Army Web Risk Assessment Cell
A team of information assurance personnel that conduct ongoing operational security and threat assessments of Army publicly accessible Web sites to ensure compliance with DOD and Army policy and best practices.

Cookie
A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. They allow user-side customization of web information. Normally, cookies will expire after a single session.

Extranet
Similar to an intranet, an extranet includes outside vendors and uses web technology to facilitate inter-business transactions, such as placing and checking orders, tracking merchandise, and making payments.

Information Assurance Vulnerability Alerts (IAVA)
Positive control mechanism that pushes alerts and advisories on IA security vulnerabilities to IA personnel. IAVA also requires the tracking of response and compliance to the messages.

Infostructure
The infostructure is defined as the shared computers, ancillary equipment, software, firmware and similar procedures, services, people, business processes, facilities and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, whether supporting Information Technology or National Security systems as defined in the Clinger-Cohen Act of 1996.

Intranet
A computer network that functions like the internet using web browser software to access and process the information that employees need, but the information and web pages are located on computers within the organization/enterprise. A firewall is usually used to block access from outside the intranet. Intranets are private web sites.

Persistent Cookies
Cookies that can be used to track users over time and across different web sites to collect personal information

Publications
Items of information that are printed or reproduced, whether mechanically or electronically, for distribution or dissemination usually to a predetermined audience.

Generally, they are directives, books, pamphlets, posters, forms, manuals, brochures, magazines, and newspapers produced in any media by or for the Army.

Third Party Cookies
Cookies placed on a user's hard drive by Internet advertising networks. The most common third-party cookies are placed by the various companies that serve the banner ads that appear across many web sites.

URL
(Uniform Resource Locator) A web address you use to tell your browser where to find a particular internet resource (e.g., file, a web page, an application, etc.). All web addresses have a URL.

Web portals
Web sites that serve as starting points to other destinations or activities on the web. Initially thought of as a "home base" type of web page, portals attempt to provide "all of your internet needs in one location." Portals commonly provide services such as e-mail, online chat forums, searching, content, newsfeeds and others.

Web site
A location on the Internet; specifically it refers to the Point of Presence (POP) location in which it resides. All web sites are referenced using a special addressing scheme called a URL. A web site can mean a single HTML file or hundreds of files placed on the net by an enterprise.

World Wide Web (WWW)
A part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces and hypertext links between different addresses—called also "Web."